Randomizing quantum states in Shatten p-norms

Kabgyun Jeong[1,*]

[1] *School of Computational Sciences,*

Korea Institute for Advanced Study,

Hoegiro 87, Dongdaemun, Seoul 130-722, Korea

(Dated: March 2, 2013)

Abstract

In this paper, we formularize a method for randomizing quantum states with respect to the Shatten p-norms in trace class.

PACS numbers: 03.67.-a, 03.67.Hk,

*Electronic address: kgjeong6@kias.re.kr

I. INTRODUCTION

Randomizing quantum states in quantum information theory has many applications in quantum communications such as super-dense coding [1], data hiding [2] and proof of the additivity violation for the classical capacity on quantum channels [3]. Following Hayden, Leung, Shor and Winter's result [2] and Dickinson and Nayak's [4], we would like to make a special formula for the randomization of all quantum states.

Let $\mathcal{B}(\mathbb{C}^d)$ be the space of (bounded) linear operators and $\mathcal{U}(d) \subset \mathcal{B}(\mathbb{C}^d)$ the unitary group on the d dimensional Hilbert space $\mathbb{C}^d$, and $\mathbf{I}$ stands for the $d \times d$ identity operator on the space. Let $\mathcal{P}(\mathbb{C}^d)$ denote the set of all *pure states* i.e., unit vectors on $\mathbb{C}^d$.

For any matrix $A \in \mathcal{B}(\mathbb{C}^d)$, let $s_1, \ldots, s_d$ denote the *singular values* of A, which are also defined by the square roots of the eigenvalues of $AA^\dagger$. Then, for all $1 \leq p \leq \infty$, the *Shatten p-norm* is defined by

$$\|A\|_p = \left(\sum_{i=1}^{d} |s_i|^p \right)^{1/p}. \tag{1}$$

For $p = 1$, the trace norm is defined by $\|A\|_1 = \mathrm{tr}\sqrt{A^\dagger A}$, that is, the sum of singular values of the matrix A. The Hilbert-Schmidt (or Frobenius) norm corresponds to the case $p = 2$ and it is defined by $\|A\|_2 = \sqrt{\mathrm{tr}A^\dagger A} = \sqrt{\sum_{i=1}^{d} s_i^2}$. Finally, for $p = \infty$, this definition should be understood as $\|A\|_\infty = \max\{s_i\}$ and same to the usual operator norm. In this reason, the Shatten p-norm can be described in trace class by $\|A\|_p = \left(\mathrm{tr}(A^\dagger A)^{p/2}\right)^{1/p}$.

For all matrix $A \in \mathcal{B}(\mathbb{C}^d)$ and $1 \leq p \leq \infty$, the Shatten p-norm always satisfies

$$\|A\|_\infty \leq \|A\|_p \leq \|A\|_1. \tag{2}$$

Also, for every $r > p \geq 1$, the following Hölder's inequality (right) holds

$$\|A\|_r \leq \|A\|_p \leq d^{\left(\frac{1}{p} - \frac{1}{r}\right)} \|A\|_r. \tag{3}$$

Furthermore, for any $A,\ B \in \mathcal{B}(\mathbb{C}^d)$, the reverse triangle inequality on p-norm holds as follows:

$$|\|A\|_p - \|B\|_p| \leq \|A - B\|_p. \tag{4}$$

Now, let's define an ε-randomizing maps with respect to the Shatten p-norm.

Definition 1. A completely positive and trace-preserving map $\mathcal{R} : \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ is *ε-randomizing* with respect to the Shatten p-norm $\|\cdot\|_p$ if, for all states $\rho \in \mathcal{B}(\mathbb{C}^d)$,

$$\left\| \mathcal{R}(\rho) - \frac{\mathbf{I}}{d} \right\|_p \leq \frac{\varepsilon}{\sqrt[p]{d^{p-1}}}. \tag{5}$$

If ε is equal to zero, the map $\mathcal{R}$ is called by completely randomizing map. Above definition of ε-randomizing map is well defined for some special cases p. Since, for the map $\mathcal{R}$ with respect to the trace norm, the ε-randomizing map is defined by the condition $\|\mathcal{R}(\rho) - \mathbf{I}/d\|_1 \leq \varepsilon$. Similarly, for $p = \infty$ case, the condition is naturally defined as $\|\mathcal{R}(\rho) - \mathbf{I}/d\|_\infty \leq \varepsilon/d$.

Remark 1. By the convexity of the Shatten p-norm, it suffices to consider the condition for all pure states.

Definition 2. A probability measure μ on $\mathcal{U}(d)$ is said to be isotropic if, for all density matrix $\rho \in \mathcal{B}(\mathbb{C}^d)$,

$$\int_{\mathcal{U}(d)} U\rho U^\dagger d\mu(U) = \frac{\mathbf{I}}{d}. \tag{6}$$

Notice that the Haar measure is also isotropic. This definition will be used to prove Lemma 3 in next section. (The log and exp functions are always taken base 2.)

II. MAIN RESULTS

We are interesting to approximating the randomizing map $\mathcal{R}$ by mapping with small cardinality of unitary operators, and reproducing the known two results [2, 4] exactly.

Theorem 1. *Let φ be a pure state in $\mathcal{P}(\mathbb{C}^d)$, and μ be the Haar measure on the unitary group $\mathcal{U}(d)$. For all $\varepsilon \geq 0$ and sufficiently large d, there exists a choice of unitaries in $\mathcal{U}(d)$, $\{U_i | 1 \leq i \leq m\}$ with $m \geq \frac{c_p \cdot d}{\varepsilon^2} \log\left(\frac{10 d^{(p-1)/p}}{\varepsilon}\right)$, which is independent μ-distributed random matrices, such that the map*

$$\mathcal{R}(\varphi) = \frac{1}{m} \sum_{i=1}^{m} U_i \varphi U_i^\dagger$$

on $\mathcal{B}(\mathbb{C}^d)$ is ε-randomizing with respect to the Shatten p-norms for all $p \geq 1$ with probability at least $1 - e^{-m}$, and c_p is an absolute constant.

Let c_1 and c_∞ be absolute constants. Notice that if $p = 1$, the map $\mathcal{R}$ is ε-randomizing with respect to the trace norm with the cardinality $m = \mathcal{O}\left(\frac{c_1 \cdot d}{\varepsilon^2} \log\left(\frac{10}{\varepsilon}\right)\right)$ in Ref. [4]. If $p = \infty$, then $m = \mathcal{O}\left(\frac{c_\infty \cdot d}{\varepsilon^2} \log\left(\frac{10d}{\varepsilon}\right)\right)$ in Ref. [2].

Since some technical lemmas are needed, we postpone the proof of Theorem 1 to the next section.

Lemma 2. *For all $r > p \geq 1$ and for any density matrix $A \in \mathcal{B}(\mathbb{C}^d)$,*

$$\left\| A - \frac{\mathbf{I}}{d} \right\|_p^r \leq d^{\frac{r-p}{p}} \|A\|_r^r - \frac{d^{\frac{r-p}{p}}}{d^p}. \tag{7}$$

Proof. It directly follows from the density matrix A and the Hölder's inequality Eq. (3). □

Lemma 3. *For a fixed pure state $\varphi \in \mathcal{B}(\mathbb{C}^d)$, let's define $Y_{[\varphi]} = \left\| \mathcal{R}(\varphi) - \frac{\mathbf{I}}{d} \right\|_p$. Then, for all $r > p \geq 1$,*

$$\mathbb{E} Y_{[\varphi]} \leq \left(\frac{\sqrt[p]{d}}{m^p} + \frac{r}{m^{p-1} \cdot \sqrt[p]{d}} \right)^{1/r}. \tag{8}$$

Proof. (i) $p = 1$ and $r = 2$ case: We note that the expectation is taken on the unitaries $\{U_i\}$, and also note that $\mathcal{R}(\varphi) = \frac{1}{m} \sum_{i=1}^m U_i \varphi U_i^\dagger$ and $Y_{[\varphi]} := \left\| \mathcal{R}(\varphi) - \frac{\mathbf{I}}{d} \right\|_1$. Then,

$$\begin{aligned} \mathbb{E} \|\mathcal{R}(\varphi)\|_2^2 &= \frac{1}{m} + \frac{1}{m^2} \sum_{i \neq j}^m \mathbb{E} \mathrm{tr}(U_i \varphi U_i^\dagger U_j \varphi U_j^\dagger) \\ &\leq \frac{1}{m} + \mathrm{tr}(\mathbb{E}_{U_i} U_i \varphi U_i^\dagger)(\mathbb{E}_{U_j} U_j \varphi U_j^\dagger) \qquad (9) \\ &= \frac{1}{m} + \mathrm{tr} \frac{\mathbf{I}}{d^2} = \frac{1}{m} + \frac{1}{d}, \end{aligned}$$

where the inequality in Eq. (9) follows from the definition of isotropic measure $\mathbb{E}_U U \varphi U^\dagger := \int_{\mathcal{U}(d)} U \varphi U^\dagger d\mu U = \frac{\mathbf{I}}{d}$. By exploiting the Cauchy-Schwartz inequality, $Y_{[\varphi]}^2 \leq d \|\mathcal{R}(\varphi)\|_2^2 - 1$, and we can find $\mathbb{E} Y_{[\varphi]}^2 \leq d \mathbb{E} \|\mathcal{R}(\varphi)\|_2^2 - 1$. (See Ref. [4].) Therefore, for sufficiently large d,

$$\mathbb{E} Y_{[\varphi]} \leq \sqrt{\mathbb{E} Y_{[\varphi]}^2} \leq \sqrt{d \mathbb{E} \|\mathcal{R}(\varphi)\|_2^2 - 1} = \sqrt{\frac{d}{m}}.$$

(ii) $p = 2$ and $r = 3$ case: Consider that $Y_{[\varphi]} = \left\| \mathcal{R}(\varphi) - \frac{\mathbf{I}}{d} \right\|_2$. Likewise the case (i), we can directly obtain the following inequality: $\mathbb{E} \|\mathcal{R}(\varphi)\|_3^3 \leq \frac{1}{m^2} + \frac{3}{md} + \frac{1}{d^2}$. Thus, from the Hölder's inequality,

$$\mathbb{E} \left\| \mathcal{R}(\varphi) - \frac{\mathbb{I}}{d} \right\|_2^3 \leq \sqrt{d} \mathbb{E} \|\mathcal{R}(\varphi)\|_3^3 - d^{-3/2} \leq \frac{\sqrt{d}}{m^2} + \frac{3}{m\sqrt{d}}.$$

Finally, for all $r > p \geq 1$, $\|A\|_\infty \leq \|A\|_r \leq \|A\|_p \leq \|A\|_1$ is true. So, the proof is completed. □

Note that $d < m \leq d^2$.

III. PROOF OF THEOREM 1

The scheme of main proof is similar to the References [2, 4]. We need to two key-lemmas known as McDiarmid's inequality and η-net argument. The first one is a large deviation estimates and the second is a method for discretization of all pure quantum states.

Lemma 4 (McDiarmid's inequality [5]). *Let $\{X_i\}_{i=1}^m$ be m independent random variables with X_i chosen in a set $\mathcal{X}$ for each i. Suppose that the measurable function $f : \mathcal{X}^m \to \mathbb{R}$ satisfies $|f(x) - f(x')| \leq c_i$ where the vectors x and x' differ only in the i-th position. Let $Y = f(X_1, X_2, \ldots, X_m)$ be the corresponding random variable. Then for any $t \geq 0$,*

$$\mathbb{P}[|Y - \mathbb{E}(Y)| \geq t] \leq 2e^{-2t^2/\sum_{i=1}^m c_i^2}. \tag{10}$$

Lemma 5 (η-net [2]). *For every $\eta > 0$ and dimension d, there exists a set N of pure states in $\mathbb{C}^d$ of cardinality $|N| \leq \left(\frac{5}{\eta}\right)^{2d}$, such that for all pure states $|\varphi\rangle \in \mathbb{C}^d$ there is $|\tilde{\varphi}\rangle \in N$ satisfying $\||\varphi\rangle\langle\varphi| - |\tilde{\varphi}\rangle\langle\tilde{\varphi}|\|_1 \leq \eta$.*

Suppose that a randomizing map $\mathcal{R}$ is realized by a unitary sequence $(U_i)_{i=1}^m$ and another map $\tilde{R}$ is consisted by $(U_1, \ldots, U_{i-1}, U_i, U_{i+1}, \ldots, U_m)$ via the function f respectively. Then,

$$\begin{aligned}\left|\left\|\mathcal{R}(\varphi) - \frac{\mathbf{I}}{d}\right\|_p - \left\|\tilde{\mathcal{R}}(\varphi) - \frac{\mathbf{I}}{d}\right\|_p\right| &\leq \|\mathcal{R}(\varphi) - \tilde{\mathcal{R}}(\varphi)\|_p \\ &= \frac{1}{m}\|U_i\varphi U_i^\dagger - \tilde{U}_i\varphi\tilde{U}_i{}^\dagger\|_p \\ &\leq \frac{2^{1/p}}{m}.\end{aligned}$$

So the McDiarmid's inequality, on positive part ($Y_{[\varphi]} - \mathbb{E}Y_{[\varphi]} > 0$), is given by

$$\mathbb{P}\left[Y_{[\varphi]} \geq t + \left(\frac{\sqrt[p]{d}}{m^p} + \frac{r}{m^{p-1} \cdot \sqrt[p]{d}}\right)^{1/r}\right] \leq e^{-\frac{mt^2}{2^{(2-p)/p}}},$$

and similarly to the negative part.

Proof of the theorem. Let the sequence $(U_i)_{i\geq 1}^m$ be i.i.d. $\mathcal{U}(d)$-valued random variables, distributed according to the isotropic measure or the Haar measure. We will show that with high probability the corresponding map $\mathcal{R}$ is ε-randomizing. The proof will be consisted of bounding the next probability by 1: For any pure state $\varphi \in \mathcal{B}(\mathbb{C}^d)$,

$$\mathbb{P}_{\forall\varphi}\left[Y_{[\varphi]} := \left\|\frac{1}{m}\sum_{i=1}^m U_i\varphi U_i^\dagger - \frac{\mathbf{I}}{d}\right\|_p \geq \frac{\varepsilon}{\sqrt[p]{d^{p-1}}}\right] < 1. \tag{11}$$

Fix a net of N and let $\tilde{\varphi}$ be the net point corresponding to φ so that

$$\|\mathcal{R}(\varphi) - \mathcal{R}(\tilde{\varphi})\|_1 = \|\varphi - \tilde{\varphi}\|_1 \leq \frac{\varepsilon}{2\sqrt[p]{d^{p-1}}}. \tag{12}$$

So, Lemma 5 provides a net with $|N| \leq \left(\frac{10d^{(p-1)/p}}{\varepsilon}\right)^{2d}$. We can then proceed as follows:

$$\begin{aligned}
\mathbb{P}_{\forall\varphi}\left[\left\|\mathcal{R}(\varphi) - \frac{\mathbf{I}}{d}\right\|_p \geq \frac{\varepsilon}{d^{(p-1)/p}}\right] &\leq \mathbb{P}_{\forall\varphi,\tilde{\varphi}}\left[\|\mathcal{R}(\varphi) - \mathcal{R}(\tilde{\varphi})\|_p + \left\|\mathcal{R}(\tilde{\varphi}) - \frac{\mathbf{I}}{d}\right\|_p \geq \frac{\varepsilon}{d^{(p-1)/p}}\right] &(13)\\
&\leq \mathbb{P}_{\forall\tilde{\varphi}}\left[\left\|\mathcal{R}(\tilde{\varphi}) - \frac{\mathbf{I}}{d}\right\|_p \geq \frac{\varepsilon}{2d^{(p-1)/p}}\right]. &(14)
\end{aligned}$$

Above Eq. (13) exploits the triangle inequality, and in the last inequality (Eq. (14)) we have used Eq. (12), that is, $\|\mathcal{R}(\varphi) - \mathcal{R}(\tilde{\varphi})\|_p \leq \|\mathcal{R}(\varphi) - \mathcal{R}(\tilde{\varphi})\|_1 = \|\varphi - \tilde{\varphi}\|_1 \leq \frac{\varepsilon}{2\sqrt[p]{d^{p-1}}}$.

Now, if we use the union bound, the net argument (Lemma 5), and by the McDiarmid's inequality (Lemma 4), then

$$\begin{aligned}
\mathbb{P}_{\forall\varphi}\left[\left\|\mathcal{R}(\varphi) - \frac{\mathbf{I}}{d}\right\|_p \geq \frac{\varepsilon}{d^{(p-1)/p}}\right] &\leq \mathbb{P}_{\forall\tilde{\varphi}}\left[\left\|\mathcal{R}(\tilde{\varphi}) - \frac{\mathbf{I}}{d}\right\|_p \geq \frac{\varepsilon}{2d^{(p-1)/p}}\right]\\
&\leq |N| \cdot \mathbb{P}_{\tilde{\varphi}}\left[\left\|\mathcal{R}(\tilde{\varphi}) - \frac{\mathbf{I}}{d}\right\|_p \geq \frac{\varepsilon}{2d^{(p-1)/p}}\right] &(15)\\
&\leq 2\left(\frac{10d^{(p-1)/p}}{\varepsilon}\right)^{2d}\\
&\quad \times \exp\left[-\frac{m}{2^{2-2/p}}\left(\frac{\varepsilon}{2d^{(p-1)/p}} - \left(\frac{d^{1/p}}{m^p} + \frac{r}{m^{p-1}d^{1/p}}\right)^{1/r}\right)^2\right].
\end{aligned}$$

The existence of the desired ε-randomizing map with respect to the Shatten p-norm is guaranteed if the above probability is bounded above by 1, which is the case if $m \geq \frac{c_p \cdot d}{\varepsilon^2}\log(\frac{10d^{(p-1)/p}}{\varepsilon})$. This completes the proof. □

Note that the inequality of Eq. (15) follows from the union bound in probability theory, and the last inequality is direct consequence of the McDiarmid's inequality. In the estimate of m, we make use of $d < m < d^2$ and $p < r$ such that

$$\left(\frac{10d^{\frac{p-1}{p}}}{\varepsilon}\right)^{2d} \exp\left[-\frac{m}{2^{2-2/p}}\left(\frac{\varepsilon}{2d^{\frac{p-1}{p}}} - \frac{2d^{1/rd}}{m^{p/r}}\right)^2\right] < 1,$$

where, for sufficiently larger d, $\left(\frac{d^{1/p}}{m^p} + \frac{r}{m^{p-1}d^{1/p}}\right)^{1/r} \leq \left(\frac{2d^{1/p}}{m^p}\right)^{1/r}$. We here fix d and select m so that $\left(\frac{\varepsilon}{2d^{p-1/p}} - \frac{2d^{1/rd}}{m^{p/r}}\right)^2 = o(\varepsilon^2)$. Then, for a constant c,

$$2d\log\left(\frac{10d^{p-1/p}}{\varepsilon}\right) < \frac{cm\varepsilon^2}{2^{2-2/p}}.$$

Thus, we have $m \geq \frac{c_p d}{\varepsilon^2} \log \frac{10 d^{p-1/p}}{\varepsilon}$, where the constant c_p is equal to $2^{4-2/p}/c$.

IV. CONCLUSIONS

In conclusion, we have obtained a formula for randomizing quantum states with respect to the Shatten p-norms on d dimensional Hilbert space. That is, there exists a choice of unitary operators in $\mathcal{U}(d)$ selected according to the Haar measure, $\{U_i\}_{i=1}^m$ with $m = \mathcal{O}(d \log(d^{(p-1)/p}/\varepsilon)/\varepsilon^2)$ such that the completely positive and trace-preserving map $\mathcal{R}(\varphi) = \frac{1}{m} \sum_{i=1}^m U_i \varphi U_i^\dagger$ on $\mathcal{B}(\mathbb{C}^d)$ is ε-randomizing with respect to the p-norm with high probability.

Acknowledgments

This work was partially supported by the IT R&D program of the Ministry of Knowledge Economy [Development of Privacy Enhancing Cryptography on Ubiquitous Computing Environment].

[1] A. Harrow, P. Hayden, and D. Leung, Phys. Rev. Lett. **92**, 187901 (2004).

[2] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Commun. Math. Phys. **250**, 371–391 (2004).

[3] M. B. Hastings, Nature Physics **5**, 255–257 (2009).

[4] P. Dickinson and A. Nayak, In AIP Conference Proceedings **864**, 18–36 (2006).

[5] C. McDiarmid, Surveys in Combinatorics **141**, 148–188 (1989).